Guía de instalación

McAfee Enterprise Security Manager 9.5.0

COPYRIGHT

Copyright © 2015 McAfee, Inc., 2821 Mission College Boulevard, Santa Clara, CA 95054, 1.888.847.8766, www.intelsecurity.com

ATRIBUCIONES DE MARCAS COMERCIALES

Intel y el logotipo de Intel son marcas comerciales registradas de Intel Corporation en EE. UU. y en otros países. McAfee y el logotipo de McAfee, McAfee Active Protection, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, McAfee Evader, Foundscore, Foundstone, Global Threat Intelligence, McAfee LiveSafe, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, McAfee Shredder, SiteAdvisor, McAfee Stinger, McAfee TechMaster, McAfee Total Protection, TrustedSource y VirusScan son marcas comerciales o marcas comerciales registradas de McAfee, Inc. o de sus empresas filiales en EE. UU. y en otros países. Los demás nombres y marcas pueden ser reclamados como propiedad de otros.

INFORMACIÓN DE LICENCIA

Acuerdo de licencia

AVISO A TODOS LOS USUARIOS: LEA DETENIDAMENTE EL ACUERDO LEGAL CORRESPONDIENTE A LA LICENCIA QUE HA ADQUIRIDO, QUE ESTIPULA LOS TÉRMINOS Y CONDICIONES GENERALES PARA EL USO DEL SOFTWARE CON LICENCIA. SI NO SABE QUÉ TIPO DE LICENCIA HA ADQUIRIDO, CONSULTE LOS DOCUMENTOS DE VENTA Y OTROS DOCUMENTOS RELACIONADOS CON LA CONCESIÓN DE LA LICENCIA O CON LA ORDEN DE COMPRA QUE ACOMPAÑAN AL PAQUETE DE SOFTWARE, O QUE HAYA RECIBIDO POR SEPARADO COMO PARTE DE LA COMPRA (POR EJEMPLO, UN MANUAL, UN ARCHIVO DEL CD DEL PRODUCTO O UN ARCHIVO DISPONIBLE EN EL SITIO WEB DESDE EL QUE DESCARGÓ EL PAQUETE DE SOFTWARE). SI NO ACEPTA TODOS LOS TÉRMINOS DESCRITOS EN EL ACUERDO, NO INSTALE EL SOFTWARE. SI PROCEDE, PUEDE DEVOLVER EL PRODUCTO A MCAFEE O AL LUGAR DONDE LO ADQUIRIÓ CON EL FIN DE OBTENER SU REEMBOLSO ÍNTEGRO.

Contenido

Prefacio **5**
Acerca de esta guía 5
Destinatarios 5
Convenciones 5
Búsqueda de documentación de productos 6

1 Introducción **7**

2 Instalación de los dispositivos McAfee ESM **9**
Preparación para la instalación de los dispositivos McAfee ESM 9
Requisitos de hardware y software 9
Inspección del embalaje y el dispositivo 10
Identificación de una ubicación para la instalación 10
Conexión e inicio de los dispositivos 11
Identificación de los tipos de conectores y equipos 12
Identificación de los cables de red 12
Identificación de los puertos de red 13

3 Configuración de los dispositivos McAfee ESM **23**
Configuración de la interfaz de red en Nitro IPS 23
Configuración de la interfaz de red en el receptor, el ELM y el ACE 24
Configuración de la interfaz de red en el DEM y el ADM 24
Configuración de la interfaz de red en el ESM 25
Configuración para IPv6 26
Inicio de sesión en la consola de McAfee ESM 26

A Acerca del modo FIPS **29**
Información sobre el modo FIPS 30
Selección del modo FIPS 30
Comprobación de integridad de FIPS 31
Adición de un dispositivo con clave aplicada en el modo FIPS 32
Copia de seguridad y restauración de información de un dispositivo en modo FIPS 32
Activación de la comunicación con varios dispositivos ESM en el modo FIPS 33
Solución de problemas del modo FIPS 35

B Requisitos de ESXi para máquinas virtuales **37**
Modelos de máquina virtual 37
División de la unidad de almacenamiento 39
Instalación de la máquina virtual 40
Configuración de la máquina virtual 40
Aplicación de una clave al dispositivo de máquina virtual 41

C Instalación de los adaptadores SAN qLogic 2460 o 2562 **43**

D Instalación del DAS **45**

E Instalación de los dispositivos en un bastidor **47**

Instalación del juego de rieles AXXVRAIL 48

Extracción del chasis 51

F Avisos normativos **53**

Índice **57**

Prefacio

Esta guía le proporcionará toda la información que necesita para trabajar con su producto McAfee.

Contenido

- *Acerca de esta guía*
- *Búsqueda de documentación de productos*

Acerca de esta guía

Esta información incluye los destinatarios de la guía, las convenciones tipográficas y los iconos utilizados, además de cómo está organizada.

Destinatarios

La documentación de McAfee se recopila y se redacta meticulosamente para el público al que va destinada.

La información de esta guía está dirigida principalmente a:

- **Administradores**: personas que implementan y aplican el programa de seguridad de la empresa.
- **Usuarios**: personas que usan el equipo en el que se está ejecutando el software y que pueden acceder a todas o algunas de sus funciones.

Convenciones

En esta guía se utilizan los siguientes iconos y convenciones tipográficas.

Título de libro, *término* o *énfasis*	Título de un libro, capítulo o tema; introducción de un nuevo término; énfasis.
Negrita	Texto que se enfatiza particularmente.
`Datos introducidos por el usuario, código, mensajes`	Comandos u otro texto que escribe el usuario; un ejemplo de código; un mensaje que aparece en pantalla.
Texto de la interfaz	Palabras de la interfaz del producto, como los nombres de opciones, menús, botones y cuadros de diálogo.
Azul hipertexto	Un vínculo a un tema o a un sitio web externo.
	Nota: Información adicional, como un método alternativo de acceso a una opción.
	Sugerencia: Sugerencias y recomendaciones.

Importante/atención: Consejo importante para proteger el sistema, la instalación del software, la red, la empresa o los datos.

Advertencia: Consejo especialmente importante para prevenir daños físicos cuando se usa un producto de hardware.

Búsqueda de documentación de productos

Una vez que se lanza un producto, la información del producto se introduce en el Centro de conocimiento online de McAfee.

Procedimiento

1 Vaya a la ficha **Centro de conocimiento** del portal McAfee ServicePortal en http://support.mcafee.com.

2 En el panel **KnowledgeBase**, haga clic en un origen de contenido:

- **Documentación del producto** para encontrar documentación del producto
- **Artículos técnicos** para encontrar artículos de la base de datos KnowledgeBase

3 Seleccione **No borrar mis filtros**.

4 Introduzca un producto, seleccione una versión y haga clic en **Buscar** para que aparezca una lista con documentos.

1 Introducción

En esta guía se explica cómo instalar y configurar los dispositivos siguientes:

- McAfee® Nitro Intrusion Prevention System (IPS)
- McAfee® Enterprise Security Manager (McAfee ESM)
- McAfee Event Receiver
- McAfee ESM/Event Receiver (ESMREC)
- McAfee Database Event Monitor (DEM)
- McAfee Application Data Monitor (ADM)
- McAfee Enterprise Log Manager (ELM)
- McAfee Advanced Correlation Editor (ACE)
- McAfee Direct Attached Storage (DAS)
- McAfee Receiver/ELM (ELMERC)
- McAfee ESM/Receiver/ELM (ESMELM)

Se encuentra dividida en dos secciones principales:

- Instalación de un dispositivo McAfee ESM, donde se proporcionan los pasos que se deben seguir a fin de inspeccionar, montar, conectar e iniciar el dispositivo.
- Configuración de un dispositivo McAfee ESM, donde se describe cómo configurar la interfaz de red para cada tipo de dispositivo, la configuración requerida para usar IPv6, cómo iniciar sesión en la consola de McAfee ESM y cómo aplicar una clave al dispositivo.

1 Introducción

2 Instalación de los dispositivos McAfee ESM

Es necesario instalar los dispositivos de McAfee para poder utilizarlos a fin de proteger la red de intrusiones o para recopilar datos de la red. Estas instrucciones de instalación se aplican a todos los modelos actuales de dispositivos McAfee ESM.

Contenido

- *Preparación para la instalación de los dispositivos McAfee ESM*
- *Conexión e inicio de los dispositivos*

Preparación para la instalación de los dispositivos McAfee ESM

Antes de instalar los dispositivos, verifique que el sistema cumpla los requisitos mínimos y que el equipamiento no se haya dañado durante el transporte. Seleccione la ubicación para configurar el equipamiento.

Requisitos de hardware y software

El sistema debe satisfacer los requisitos mínimos en cuanto a hardware y software.

Requisitos del sistema

- Procesador: clase P4 (no Celeron) o superior (Mobile/Xeon/Core2, Corei3/5/7), o bien AMD clase AM2 o superior (Turion64/Athlon64/Opteron64, A4/6/8)
- RAM: 1,5 GB
- Sistema operativo Windows: Windows 2000, Windows XP, Windows 2003 Server, Windows Vista, Windows 2008 Server, Windows Server 2012, Windows 7, Windows 8, Windows 8.1
- Navegador: Internet Explorer 7.x o posterior, Mozilla FireFox 3.0.0.0 o posterior, Google Chrome 12.0.742.91 o posterior
- Flash Player: versión 11.2.x.x o posterior

Las funciones de ESM emplean ventanas emergentes al cargar o descargar archivos. Desactive el bloqueador de ventanas emergentes para las direcciones IP o el nombre de host de su ESM.

Requisitos de la máquina virtual

- Procesador: de 8 núcleos y 64 bits, Dual Core2/Nehalem o superior, o bien AMD Dual Athlon64/ Dual Opteron64 o superior
- RAM: depende del modelo (4 GB o más)

- Espacio en disco: depende del modelo (250 GB o más)
- ESXi 5.0 o posterior
- Aprovisionamiento grueso o fino: debe decidir los requisitos de disco duro necesarios para el servidor. El requisito mínimo es de 250 GB, a menos que la máquina virtual adquirida cuente con más. Consulte las especificaciones correspondientes a su máquina virtual.

La máquina virtual de ENMELM hace uso de diversas funciones que requieren CPU y RAM. Si el entorno ESXi comparte los requisitos de CPU/RAM con otras máquinas virtuales, el rendimiento de la máquina virtual ENMELM se verá afectado. Asegúrese de incluir la capacidad de CPU y RAM necesaria de acuerdo con los requisitos.

Inspección del embalaje y el dispositivo

Antes de instalar el equipamiento, asegúrese de que no existan signos de daños o manipulación.

Procedimiento

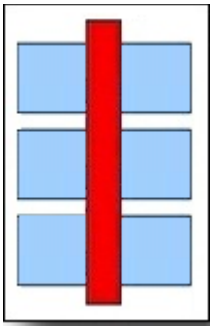
1 En cuanto reciba el dispositivo, inspeccione el embalaje y el propio dispositivo en busca de signos de daños o manipulación incorrecta.

> Si va a realizar una instalación FIPS, inspeccione la cinta de embalar que protege el contenedor de envío, donde los signos de manipulación serían evidentes. Si existen signos de manipulación, póngase en contacto con el Soporte de McAfee inmediatamente a fin de recibir instrucciones y no instale el producto.

2 Verifique que todos los elementos indicados en el albarán estén presentes en el paquete.

3 Si va a llevar a cabo una instalación FIPS, localice el sello a prueba de manipulación dentro del paquete de accesorios incluido en el contenedor de envío. Aplique el sello de forma que bloquee por completo los puertos USB, evitando así su uso sin que queden pruebas de la manipulación (véase el Diagrama 1).

Diagrama 1: Colocación del tercer sello a prueba de manipulación.



Póngase en contacto con el Soporte de McAfee de inmediato si no está completamente satisfecho con la inspección.

Identificación de una ubicación para la instalación

Es necesario analizar la red existente e identificar una ubicación de red y una ubicación física para el dispositivo. La correcta selección de la ubicación es importante para poder hacer un uso eficaz de los dispositivos.

A la hora de seleccionar una ubicación para sus dispositivos:

- Instale su dispositivo ESM en una ubicación en la red donde pueda administrar los dispositivos y resulte accesible para cualquier sistema que acceda a ESM. Si la comunicación directa no es posible entre los dispositivos gestionados por el ESM o los sistemas que ejecutan el ESM, deberá configurar la red de forma que se enrute el tráfico de red entre ellos.
- Coloque el dispositivo Nitro IPS entre la parte de confianza y la parte no de confianza de la red. La parte de confianza es la que se quiere proteger, mientras que la parte no de confianza es la que se pretende dejar sin protección. Por ejemplo, podría colocar el dispositivo Nitro IPS entre el firewall (parte no fiable) y el conmutador (parte de confianza). Como las configuraciones de red varían en gran medida, la ubicación seleccionada dependerá de los requisitos de seguridad y del entorno de red concretos.

  Este equipo está destinado a la instalación en una ubicación con acceso restringido.

- Los dispositivos correspondientes al receptor y el DEM deben resultar accesibles para los dispositivos que supervisan. Si la comunicación directa no resulta posible, es necesario configurar la red para permitir el correcto enrutamiento del tráfico de red entre ellos.

Conexión e inicio de los dispositivos

Tras inspeccionar el dispositivo e identificar la ubicación de instalación preferida, lleve a cabo los pasos incluidos en esta sección a fin de instalarlo.

Procedimiento

1 Monte el dispositivo.

Para proteger el dispositivo y el cableado frente a daños o desconexiones accidentales, monte el dispositivo en un bastidor (véase *Apéndice F - Instalación del juego de rieles AXXVRAIL*).

a Prepare un espacio para el dispositivo en la ubicación de montaje.

b Monte el dispositivo de forma segura en la ubicación seleccionada.

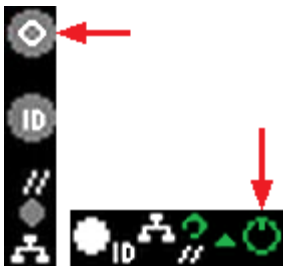
2 Conecte la fuente de alimentación al dispositivo. Instale y conecte a tierra de forma adecuada el equipo de acuerdo con este manual de instrucciones y con las normativas nacionales, regionales y locales.

Se recomienda encarecidamente conectar todos los dispositivos ESM a un sistema de alimentación ininterrumpida (SAI). Los cables y módulos de alimentación redundantes funcionando en condiciones normales equilibran la carga a través del diseño paralelo, lo cual resulta en un sistema de alimentación fiable. Ya que el dispositivo Nitro IPS está en línea, se debe conectar a un SAI.

3 Inicie el dispositivo.

a Conecte el cable sin encenderlo y asegúrese de que pase el tráfico.

b Encienda el dispositivo.



4 Seleccione el cable de red.

5 Conecte los cables a los puertos tanto de confianza como no fiables. Si va a conectar cables de fibra, retire las cubiertas de los cables y los conectores de red únicamente cuando esté listo para realizar la conexión.

6 Verifique la conectividad del dispositivo; para ello, haga ping desde el lado de confianza de la red hasta una dirección IP válida del lado no fiable.

Véase también

Identificación de los tipos de conectores y equipos en la página 12
Identificación de los cables de red en la página 12
Identificación de los puertos de red en la página 13

Identificación de los tipos de conectores y equipos

Es posible conectar el dispositivo Nitro IPS a la red mediante conectores de cobre o fibra, según el modelo del dispositivo.

Tabla 2-1 Tipo de conexión por dispositivo

Modelo de Nitro IPS	Tipo de conector
TX	RJ-45 (cobre)
SX	LC multimodo (fibra)
LX	LC de modo único (fibra)

Conecte los dispositivos correspondientes al ESM, el receptor y el DEM a la red mediante conectores de cobre, e identifique los cables de cobre o fibra por medio de los conectores. El cable de cobre CAT5 dispone de conectores RJ-45 (1), mientras que el cable de fibra LC emplea conectores de fibra (2).

Se recomienda utilizar CAT5 o superior para la conexión de cobre. En el caso de una conexión Gigabit, se recomienda el uso de CAT5e.

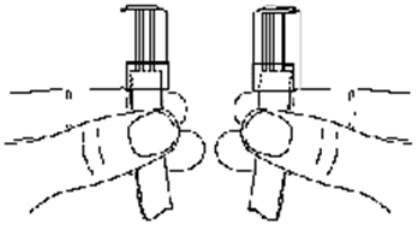
Tipo de equipo

Existen dos tipos de equipos que se pueden conectar a los dispositivos ESM: equipo de terminación del circuito de datos (ETCD) y equipo terminal de datos (ETD). Los firewalls y enrutadores son ETD, mientras que los conmutadores son ETCD. Los dispositivos ESM son ETD.

Identificación de los cables de red

Si su dispositivo emplea una conexión de fibra, deberá seleccionar los cables de fibra y conectarlos a los puertos. Si su dispositivo emplea una conexión de cobre, recurra a un cable de cobre de conexión directa o a un cable de cobre cruzado.

Para conectar el puerto RJ-45 de un dispositivo ESM al ETCD, utilice un cable directo. Para conectar con un ETD, utilice un cable cruzado. Para distinguir un cable directo de un cable cruzado, sujete ambos extremos del cable como se indica:



En un cable directo, los hilos de colores presentan la misma secuencia en ambos lados. En un cable cruzado, el primer hilo de color (extremo izquierdo) de un lado es del mismo color que el tercer hilo del otro extremo del cable.

Identificación de los puertos de red

Tras identificar los cables necesarios para la red, identifique los puertos del dispositivo de McAfee a los que conectará esos cables.

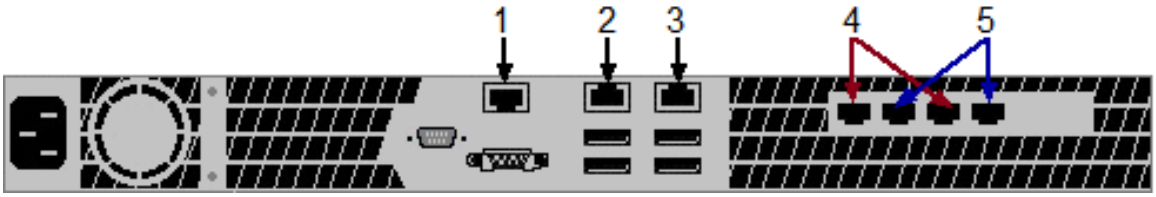
Desactive siempre cualquier fuente de láser antes de inspeccionar los conectores de fibra, los componentes ópticos o los receptáculos de conexión. Los conectores o los cables de fibra conectados podrían emitir radiación láser de fibra óptica. No mire directamente ningún equipo de fibra óptica. Coloque siempre un tapón protector en los conectores de fibra sin conectar.

Los dispositivos contienen puertos de administración, así que se pueden administrar desde McAfee ESM. Además, los dispositivos Nitro IPS y ADM contienen puertos de confianza y no fiables para conectar el dispositivo a los lados de confianza y no fiables de la red.

A fin de identificar tanto los puertos de administración como los puertos de confianza y no de confianza de todos los dispositivos, consulte esta tabla.

Tipo de dispositivo	Número de modelo	Figura
ACE	ACE-2600 o 3450	2-8
ADM	APM-1250, 1260	2-1
	APM-3450, 3460	2-3
DEM	DSM-2600 o 3450	2-3
	DSM-4600	2-4
ELM	ELM-4600, 5600 o 6000	2-8
ELM/Event Receiver	ELMERC-2600, 3450 o 4600	2-8
ESM/ELM	ENMELM- 4600, 5600 o 6000	2-8
ESM o combinación ESM/Event Receiver	ETM-5600, 6000, X4 o X6	2-8
	DAS-10, 25, 50 o 100	2-9
IPS	NTP-1250	2-2
	NTP-2600, 3450-4BTX	2-3
	NTP-2600, 3450-8BTX	2-4
	NTP-2600, 3450-4BSX	2-5

Tipo de dispositivo	Número de modelo	Figura
	NTP-3450-2BSX	2-6
McAfee Reporter	ERU-5600	2-8
Event Receiver	ERC-1250,1260	2-2
	ERC-2600, 3450 o 4600	2-7
Receptor de disponibilidad alta	1U HA - ERC-1250-HA, 1260-HA	2-10, 2-11
	2U HA - ERC-2600 o 4600-HA	2-12, 2-13



1 IPMI

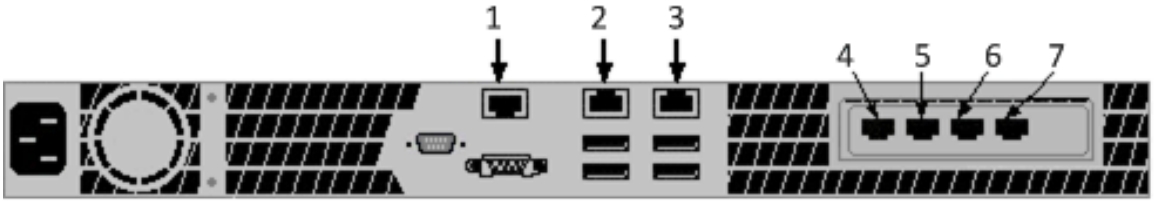
2 Admin. 2

3 Admin. 1

4 De confianza

5 No fiables

Figura 2-1 NTP-1250



1 IPMI

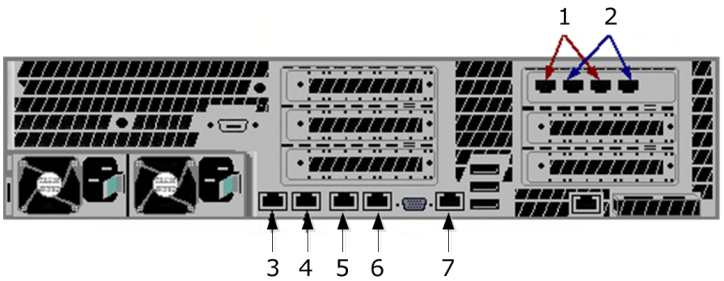
2 Admin. 2

3 Admin. 1

En el caso de los dispositivos APM-1250 y 1260, los puertos 4-7 son puertos de recopilación (analizador de protocolos o sniffer), no puertos de administración.

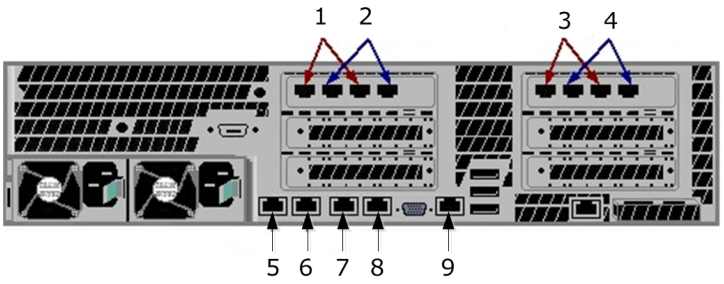
En el caso de los dispositivos ERC-1250, los puertos 4-7 son puertos de administración adicionales.

Figura 2-2 ERC-1250, APM-1250, 1260



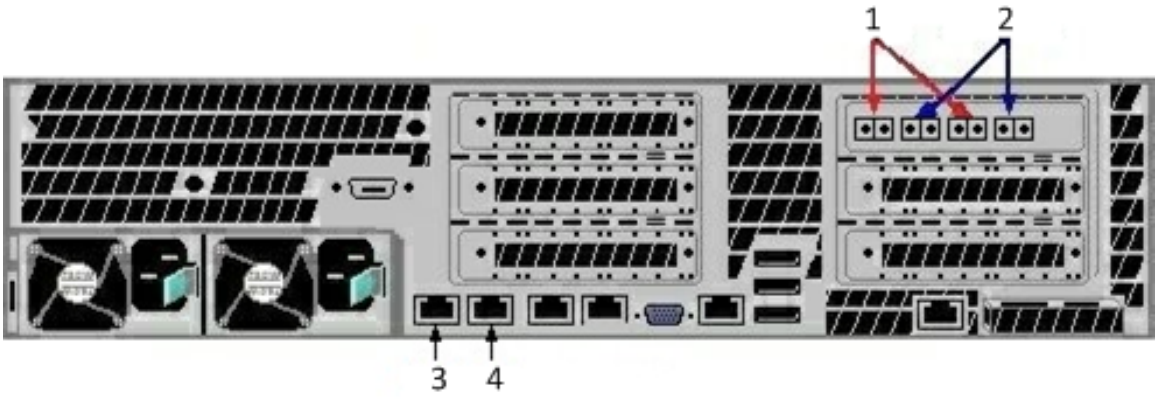
1 De confianza
2 No fiables
3 Admin. 1
4 Admin. 2
5 Sin utilizar
6 Sin utilizar
7 Sin utilizar

Figura 2-3 NTP-2600/3450-4BTX, 3460



1 De confianza
2 No fiables
3 De confianza
4 No fiables
5 Admin. 1
6 Admin. 2
7 Sin utilizar
8 Sin utilizar
9 Sin utilizar

Figura 2-4 NTP-2600/3450-8BTX, DSM-4600

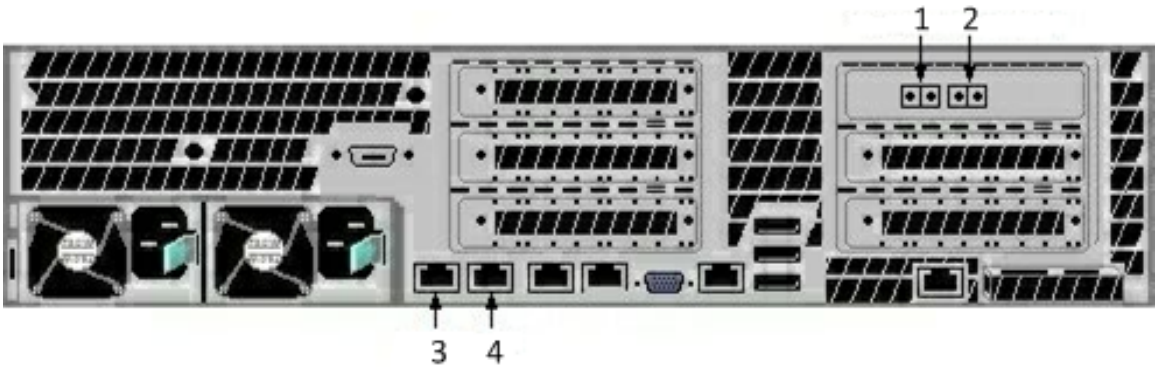


1 De confianza
2 No fiables

3 Admin. 1

4 Admin. 2

Figura 2-5 NTP-2600/3450-4BSX



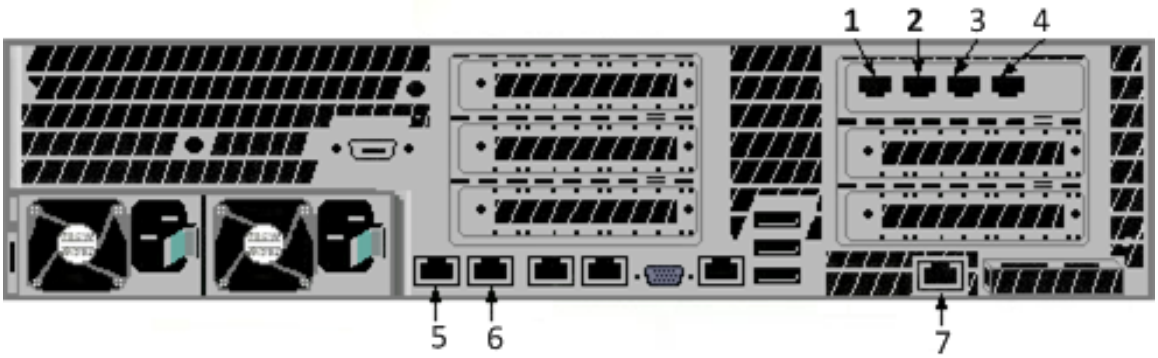
1 De confianza

2 No fiables

3 Admin. 1

4 Admin. 2

Figura 2-6 NTP-3450-2BSX



1 NIC IPMI

2 Latido

5 Admin.

6 Datos

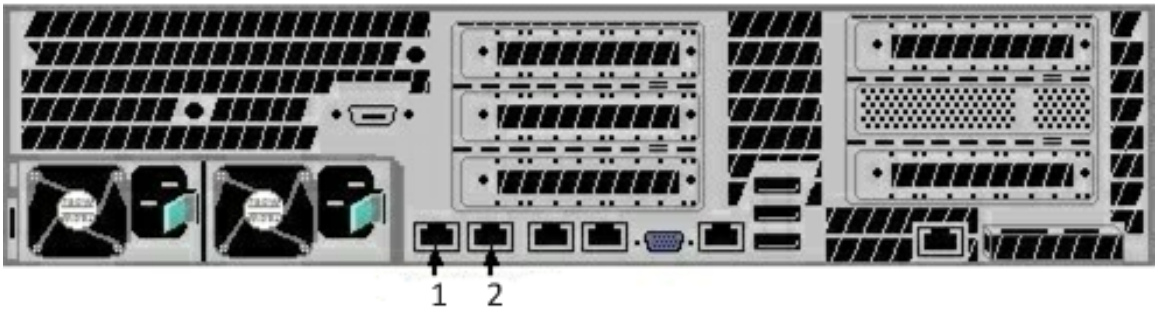
3 Admin. 2

4 Admin. 3

7 IPMI

En el caso de los dispositivos DSM-2600/3450 y APM-3450/3460, los puertos 4-7 son puertos de recopilación (analizador de protocolos o sniffer), no puertos de administración.

Figura 2-7 ERC-2600/3450/4600, DSM-2600/3450 y APM-3450/3460



1 Admin. 1

2 Admin. 2

Figura 2-8 ETM-5600/6000/X4/X6, ELMERC-2600/3450/4600, ELM-4600/5600/6000, ACE-2600/3450, ENMELM-4600/5600/6000, ERU-5600

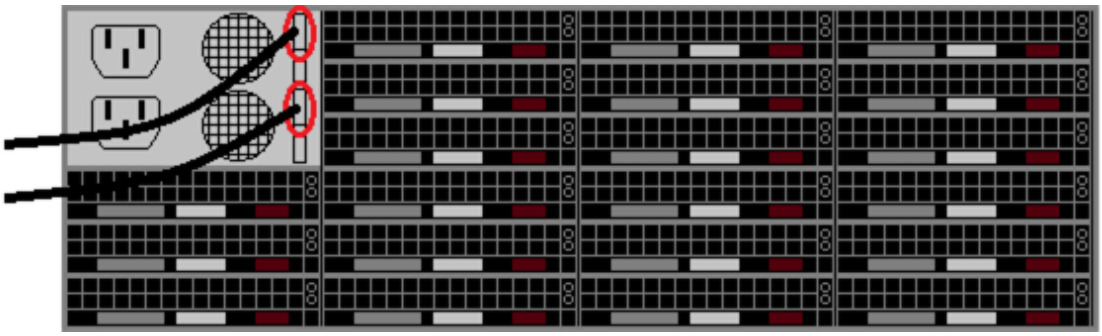
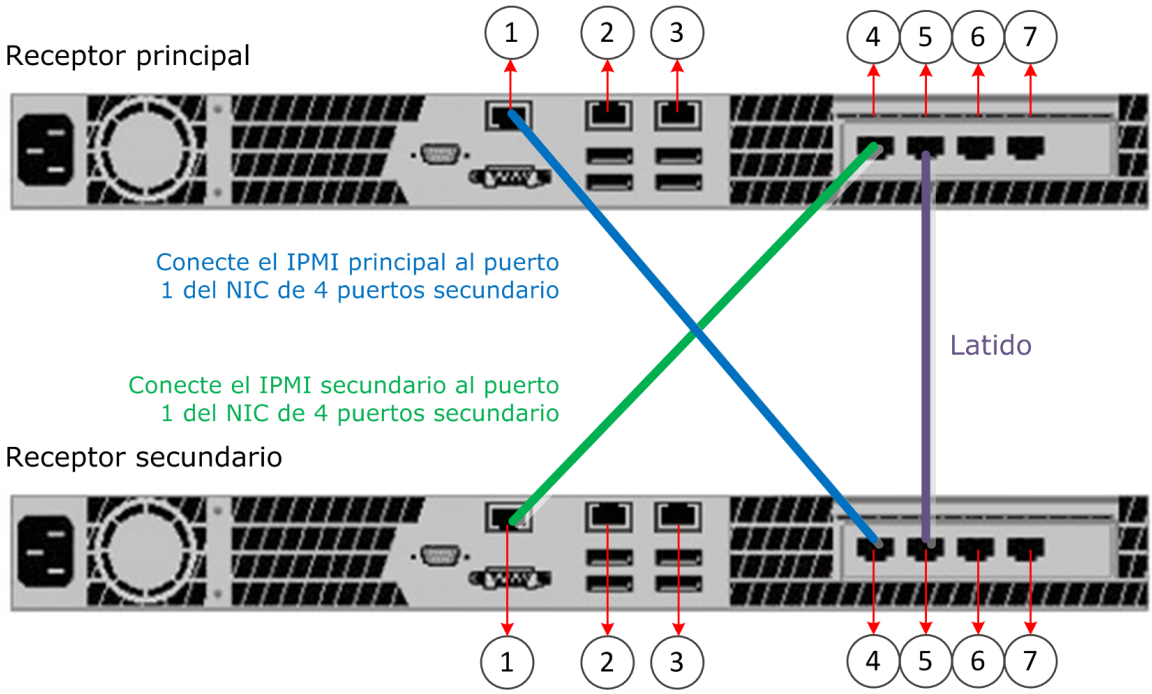
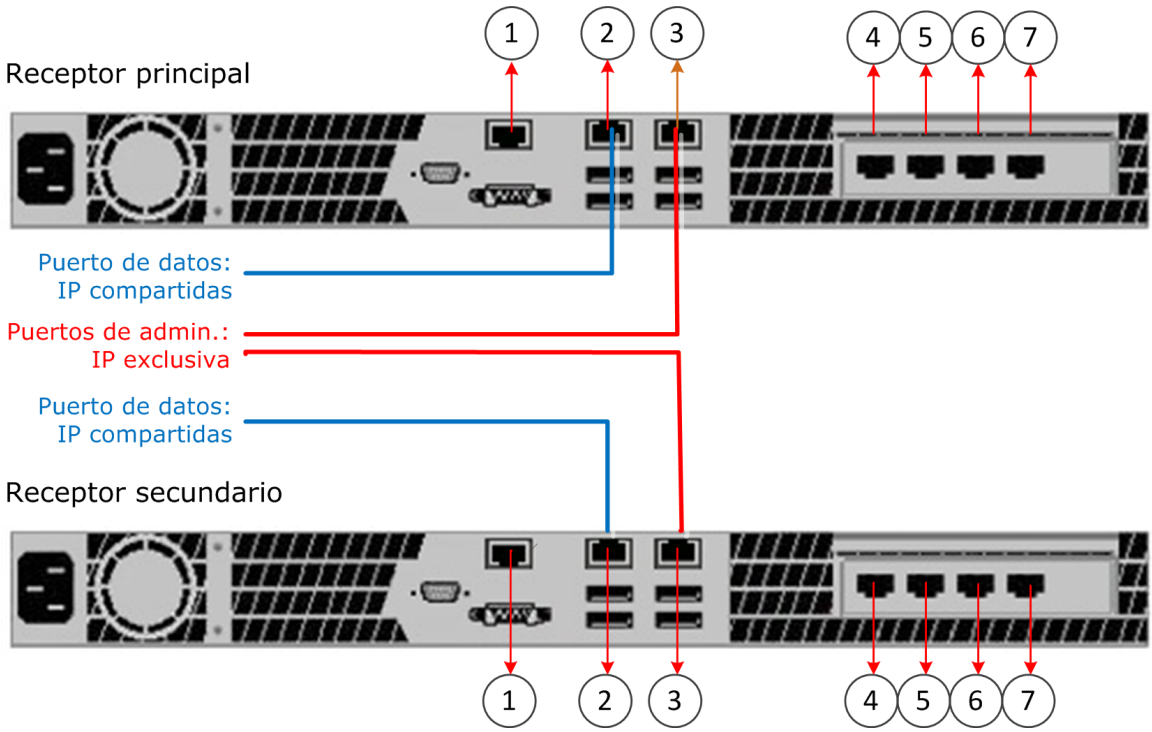


Figura 2-9 Cables de datos del DAS



1 IPMI principal
2 Admin. 2
3 Admin. 1
4 IPMI secundario
5 Latido (Heartbeat)
6 Admin. 3

Figura 2-10 Paso 1: Crear una conexión entre receptores de disponibilidad alta 1U



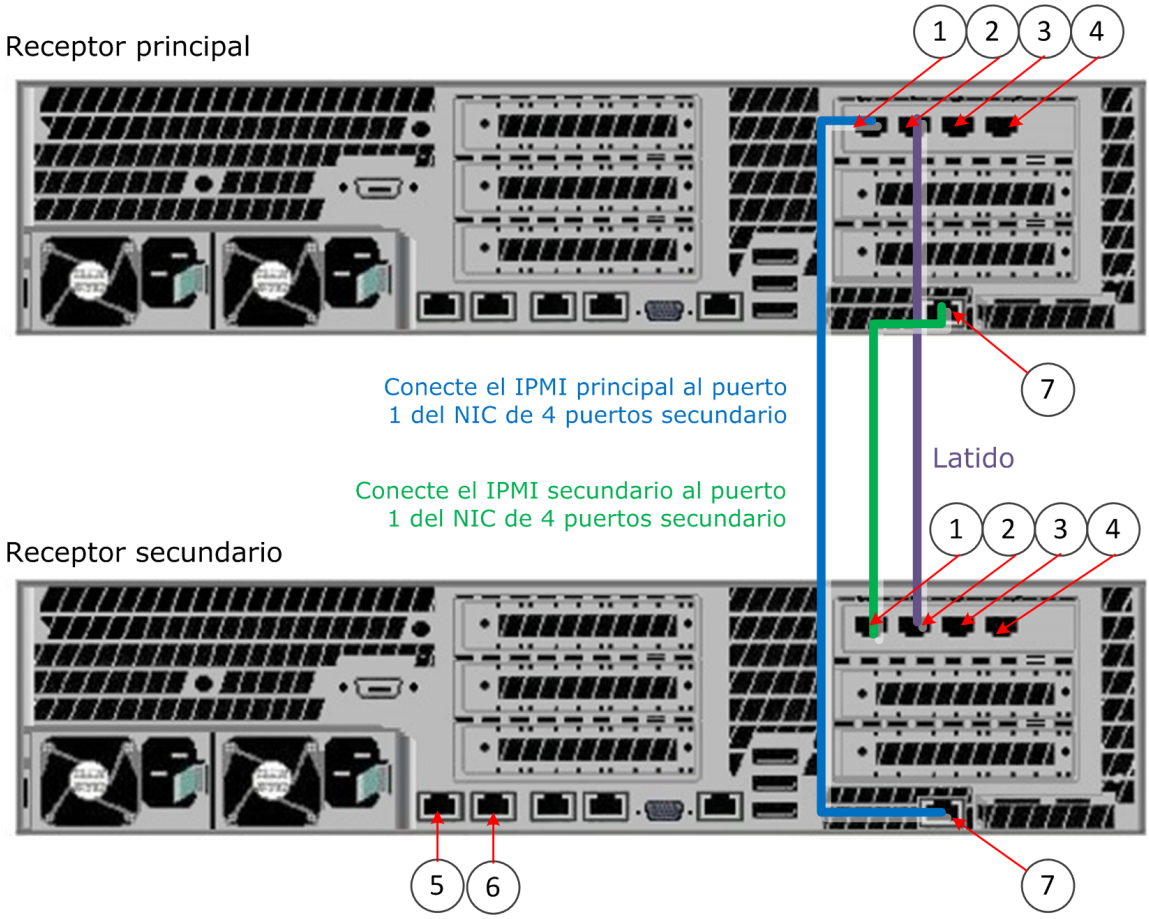
1 IPMI
2 Admin. 2 (eth1)
5 Admin. 4 (eth3)
6 Admin. 5 (eth4)

3 Admin. 1 (eth0)

4 Admin. 3 (eth2)

7 Admin. 6 (eth5)

Figura 2-11 Paso 2: Conectar los receptores de disponibilidad alta 1U al conmutador/enrutador de red



1 IPMI

2 Admin. 2 (eth1)

5 Admin. 4 (eth3)

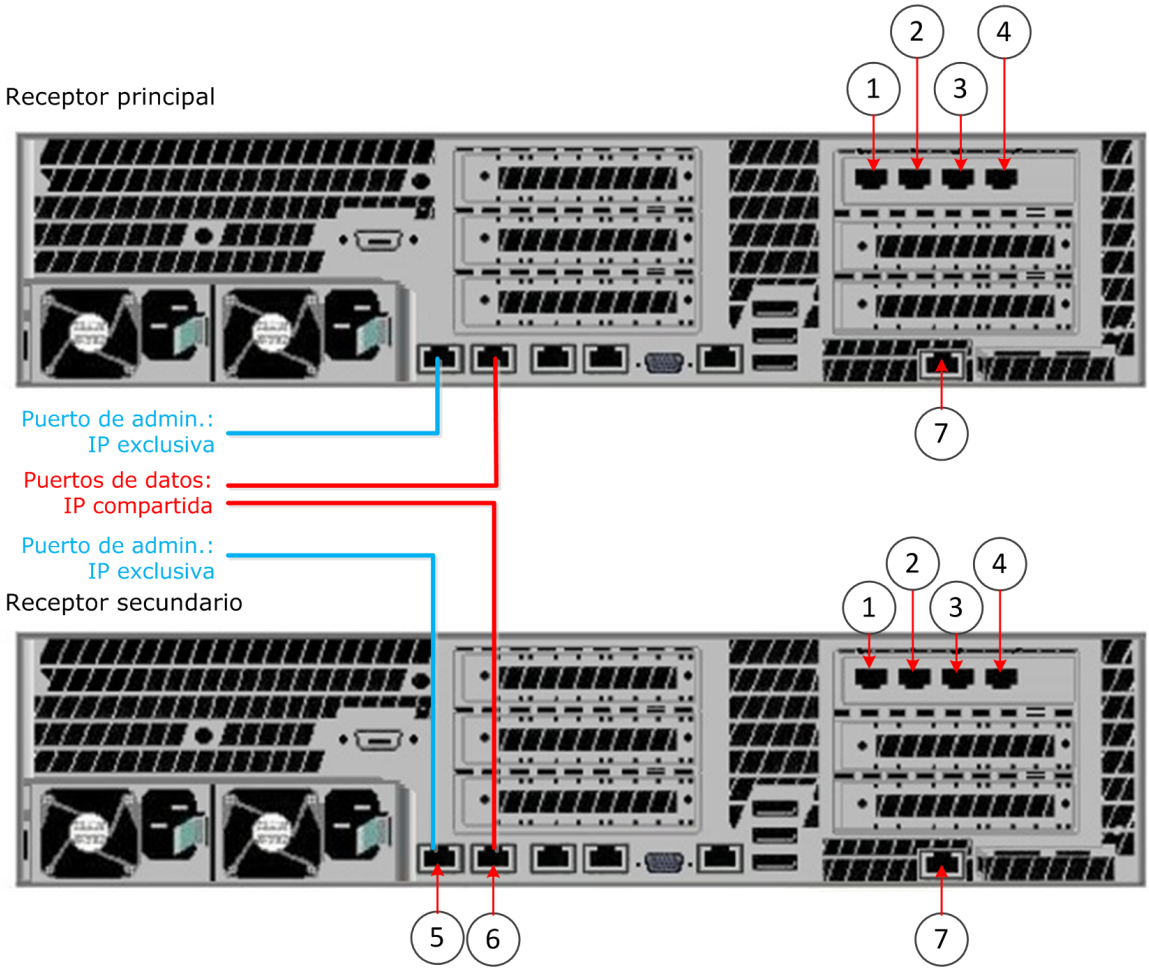
6 Admin. 5 (eth4)

3 Admin. 1 (eth0)

4 Admin. 3 (eth2)

7 Admin. 6 (eth5)

Figura 2-12 Paso 1: Crear una conexión entre receptores de disponibilidad alta 2U



1 IPMI

2 Admin. 2 (eth1)

3 Admin. 1 (eth0)

4 Admin. 3 (eth2)

5 Admin. 4 (eth3)

6 Admin. 5 (eth4)

7 Admin. 6 (eth5)

Figura 2-13 Paso 2: Conectar los receptores de disponibilidad alta 2U al conmutador/enrutador de red

Véase también

Identificación de una ubicación para la instalación en la página 10

3 Configuración de los dispositivos McAfee ESM

La configuración de los dispositivos es crucial para el correcto funcionamiento. Con este fin, es necesario configurar IPv6 y la interfaz de red para cada tipo de dispositivo, además de iniciar sesión en McAfee ESM.

Contenido

- *Configuración de la interfaz de red en Nitro IPS*
- *Configuración de la interfaz de red en el receptor, el ELM y el ACE*
- *Configuración de la interfaz de red en el DEM y el ADM*
- *Configuración de la interfaz de red en el ESM*
- *Configuración para IPv6*
- *Inicio de sesión en la consola de McAfee ESM*

Configuración de la interfaz de red en Nitro IPS

Siga estos pasos para configurar la información de IP.

Antes de empezar

Encienda el dispositivo Nitro IPS y asegúrese de que el proceso de arranque haya finalizado. Conecte un monitor y un teclado al dispositivo.

Procedimiento

1. Pulse **Alt + F1** para acceder a la pantalla LCD y, después, pulse **Esc** dos veces.
2. Desplácese hacia abajo hasta **MGT IP Conf** (Conf. IP admin.) y pulse **Intro**.
3. Seleccione **Mgt 1** (Admin. 1) y pulse **Intro**.
4. En el menú **Active** (Activa), seleccione **IP Address** (Dirección IP) y pulse **Intro**.
5. Establezca el valor y pulse **Intro**.
6. Desplácese hacia abajo hasta **Netmask** (Máscara de red) y defina el valor.
7. Desplácese hacia abajo hasta **Done** (Listo) y pulse **Intro**.
8. Desplácese hacia abajo hasta **Gateway** (Gateway) y pulse **Intro**.
9. Establezca la dirección del gateway, desplácese hacia abajo hasta **Done** (Listo) y pulse **Intro**.

10 Desplácese hacia abajo hasta **Port Number** (Número de puerto), establezca el valor y pulse **Intro**.

Tome nota del nuevo número de puerto e introdúzcalo a la hora de aplicar la clave al dispositivo. Si el sistema funciona en el modo FIPS, no cambie el número del puerto de comunicación.

11 Desplácese hacia abajo hasta **Save Changes** (Guardar cambios) y pulse **Intro**.

Configuración de la interfaz de red en el receptor, el ELM y el ACE

Siga estos pasos para configurar la interfaz de red en un dispositivo Event Receiver, ELM o ACE.

Antes de empezar

Conecte un monitor y un teclado al dispositivo.

Procedimiento

1 Pulse **Alt + F1** para acceder a la pantalla LCD, pulse dos veces **Esc**, desplácese hacia abajo hasta **MGT IP Conf** (Conf. IP admin.) y pulse **Intro**.

2 Seleccione **Mgt 1** (Admin. 1) y pulse **Intro**; a continuación, seleccione **IP Address** (Dirección IP) y pulse **Intro**.

3 Establezca el valor y pulse **Intro**.

4 Desplácese hacia abajo hasta **Netmask** (Máscara de red) y defina el valor.

5 Desplácese hacia abajo hasta **Done** (Listo) y pulse **Intro**.

6 Desplácese hacia abajo hasta **Gateway** (Gateway) y pulse **Intro**.

7 Establezca la dirección del gateway, desplácese hacia abajo hasta **Done** (Listo) y pulse **Intro**.

8 Desplácese hacia abajo hasta **DNS 1** (DNS 1), pulse **Intro** y establezca el valor.

9 Desplácese hacia abajo hasta **Done** (Listo) y pulse **Intro**.

10 Si está usando el modo FIPS, desplácese hacia abajo hasta **Port Number** (Número de puerto), cambie el valor si procede y pulse **Intro**.

Tome nota del nuevo número de puerto. Introdúzcalo en el momento de aplicar la clave al dispositivo. No cambie el puerto de comunicación TCP.

11 Desplácese hacia abajo hasta **Save Changes** (Guardar cambios) y pulse **Intro**.

Configuración de la interfaz de red en el DEM y el ADM

Siga estos pasos para configurar la interfaz de red en un dispositivo DEM o ADM.

Antes de empezar

Conecte un monitor y un teclado al dispositivo.

Procedimiento

1 Pulse **Alt + F1** para acceder a la pantalla LCD y, después, pulse **Esc** dos veces.

2 Desplácese hacia abajo hasta **MGT IP Conf** (Conf. IP admin.) y pulse **Intro**.

3 Seleccione **Mgt 1** (Admin. 1) y pulse **Intro**.

4 En el menú **Active** (Activa), seleccione **IP Address** (Dirección IP) y pulse **Intro**.

5 Establezca el valor y pulse **Intro**.

6 Desplácese hacia abajo hasta **Netmask** (Máscara de red) y defina el valor.

7 Desplácese hacia abajo hasta **Done** (Listo) y pulse **Intro**.

8 Desplácese hacia abajo hasta **Gateway** (Gateway) y pulse **Intro**.

9 Establezca la dirección del gateway, desplácese hacia abajo hasta **Done** (Listo) y pulse **Intro**.

10 Si está usando el modo FIPS, desplácese hacia abajo hasta **Port Number** (Número de puerto), cambie el valor si procede y pulse **Intro**.

Tome nota del nuevo número de puerto e introdúzcalo a la hora de aplicar la clave al dispositivo. No cambie el puerto de comunicación TCP.

11 Desplácese hacia abajo hasta **Save Changes** (Guardar cambios) y pulse **Intro**.

Configuración de la interfaz de red en el ESM

Siga estos pasos para configurar la interfaz de red en un ESM.

Antes de empezar

Encienda el ESM y asegúrese de que el proceso de inicio finalice antes de conectar un monitor y un teclado al dispositivo.

Procedimiento

1 Pulse **Alt + F1** para acceder a la pantalla LCD, pulse dos veces **Esc**, desplácese hacia abajo hasta **MGT IP Conf** (Conf. IP admin.) y pulse **Intro**.

2 Seleccione **Mgt 1** (Admin. 1) y pulse **Intro**; a continuación, seleccione **IP Address** (Dirección IP) y pulse **Intro**.

3 Establezca el valor y pulse **Intro**.

4 Desplácese hacia abajo hasta **Netmask** (Máscara de red) y defina el valor.

5 Desplácese hacia abajo hasta **Done** (Listo) y pulse **Intro**.

6 Desplácese hacia abajo hasta **Gateway** (Gateway) y pulse **Intro**.

7 Establezca la dirección del gateway, desplácese hacia abajo hasta **Done** (Listo) y pulse **Intro**.

8 Desplácese hacia abajo hasta **DNS 1** (DNS 1), pulse **Intro** y establezca el valor.

9 Desplácese hacia abajo hasta **Done** (Listo) y pulse **Intro**.

10 Desplácese hacia abajo hasta **Save Changes** (Guardar cambios) y pulse **Intro**.

Configuración para IPv6

Si desea utilizar IPv6 en cualquiera de los dispositivos y la red admite la configuración automática sin estado de IPv6, configure el sistema para la administración de IPv6.

Antes de empezar

Conecte un monitor y un teclado al dispositivo.

A fin de configurar manualmente una dirección para el ESM, véase la sección *Configuración de la red* de la *Guía del producto de McAfee Enterprise Security Manager*. Si desea configurar de forma manual una dirección para cada tipo de dispositivo, consulte la sección *Interfaces* correspondiente al dispositivo en cuestión.

Procedimiento

1 Pulse **Alt + F1** para acceder a la página **LCD** y, después, pulse **Esc** dos veces.

2 Desplácese hacia abajo hasta **IPv6 Config** (Configuración de IPv6) y pulse **Intro**.

3 Seleccione **Mgt 1** (Admin. 1) y pulse **Intro**.

4 Desplácese hacia abajo hasta **Save** (Guardar) y pulse **Intro**.

5 Para localizar la dirección IPv6 configurada automáticamente, haga lo siguiente:

   a Inicie el dispositivo y espere a que se cargue el menú.

   b Desplácese hacia abajo hasta **MGT IP Conf** (Config. IP admin.) y pulse **Intro**.

   c Desplácese hacia abajo hasta **IPv6 Global** (Global de IPv6) y pulse **Intro**.

   d Confirme la dirección IPv6 y, después, pulse **Intro** para volver al menú.

   e Desplácese hacia abajo hasta **Done** (Listo) y pulse **Intro**.

   f Desplácese hacia abajo hasta **Cancel Changes** (Cancelar cambios) y pulse **Intro**.

Inicio de sesión en la consola de McAfee ESM

Después de instalar y configurar el ESM y los dispositivos, puede iniciar sesión en la consola para empezar a configurar el sistema y las opciones de los dispositivos.

Antes de empezar

Verifique si está obligado o no a utilizar el sistema en el modo FIPS (véase el Paso 5).

Procedimiento

1 Abra un navegador web en el equipo cliente y diríjase a la dirección IP establecida al configurar la interfaz de red.

2 Haga clic en **Inicio de sesión**, seleccione el idioma para la consola y escriba el nombre de usuario y la contraseña predeterminados.

   - Nombre de usuario predeterminado: `NGCP`
   - Contraseña predeterminada: `security.4u`

3 Haga clic en **Inicio de sesión**, lea el **Acuerdo de licencia** de usuario final y haga clic en **Aceptar**.

4 Cuando se le solicite, cambie el nombre de usuario y la contraseña; después, haga clic en **Aceptar**.

5 Indique si desea activar o no el modo FIPS.

> En caso de estar obligado a trabajar en el modo FIPS, deberá activarlo la primera vez que inicie sesión, de forma que toda comunicación futura con los dispositivos de McAfee se produzca en el modo FIPS. No active el modo FIPS si no está obligado a hacerlo. Para obtener más información sobre FIPS, consulte el *Apéndice A*.

6 Siga las instrucciones que aparecerán a fin de obtener el nombre de usuario y la contraseña, que son necesarios para acceder a las actualizaciones de reglas.

7 Lleve a cabo la configuración inicial de ESM:

- **a** Seleccione el idioma que se utilizará para los registros del sistema.
- **b** Seleccione la zona horaria donde se encuentra el ESM y el formato de fecha para utilizarlos con esta cuenta; después, haga clic en **Siguiente**.
- **c** Defina la configuración en las cinco páginas del asistente **Configuración inicial de ESM**; haga clic en el icono **Ayuda** en cada una de las páginas para obtener instrucciones.

8 Haga clic en **Aceptar**.

Ya está todo listo para aplicar una clave a los dispositivos y configurarlos. Véase la *Guía del producto de McAfee Enterprise Security Manager*.

A

Acerca del modo FIPS

FIPS (del inglés Federal Information Processing Standards, estándares federales de procesamiento de la información) son estándares desarrollados y anunciados públicamente por el gobierno de los Estados Unidos sobre el procesamiento de la información. Si está obligado a cumplir estos estándares, deberá utilizar este sistema en el modo FIPS.

El modo FIPS se debe seleccionar la primera vez que se inicia sesión en el sistema y no es posible cambiarlo posteriormente.

Contenido

- *Información sobre el modo FIPS*
- *Selección del modo FIPS*
- *Comprobación de integridad de FIPS*
- *Adición de un dispositivo con clave aplicada en el modo FIPS*
- *Solución de problemas del modo FIPS*

Información sobre el modo FIPS

Debido a las normativas de FIPS, algunas funciones de ESM no están disponibles, algunas funciones disponibles no son conformes y otras funciones solo están disponibles en el modo FIPS. Estas funciones se indican a lo largo del presente documento y se enumeran aquí.

Estado de función	Descripción
Funciones eliminadas	• Receptores de disponibilidad alta. • Terminal de interfaz gráfica de usuario. • Capacidad de comunicación con el dispositivo mediante el protocolo SSH. • En la consola del dispositivo, el shell raíz se sustituye por un menú de administración de dispositivos.
Funciones solo disponibles en el modo FIPS	• Existen cuatro funciones de usuario que no coinciden parcialmente: **Usuario**, **Usuario avanzado**, **Administrador de auditorías** y **Administrador de claves y certificados**. • Todas las páginas de **Propiedades** cuentan con una opción **Prueba automática de FIPS** que permite verificar si el sistema funciona correctamente en el modo FIPS. • Si se produce un error de FIPS, se agrega un indicador de estado al árbol de navegación del sistema para reflejar este fallo. • Todas las páginas de **Propiedades** tienen una opción **Ver** que, al hacer clic en ella, abre la página **Token de identidad de FIPS**. Esta página muestra un valor que se debe comparar con el valor mostrado en las secciones del documento mencionadas para asegurarse de que no hay riesgos en relación con FIPS. • En **Propiedades del sistema** | **Usuarios y grupos** | **Privilegios** | **Editar grupo**, la página incluye el privilegio **Prueba automática de cifrado FIPS**, que otorga a los miembros del grupo la autorización para ejecutar pruebas automáticas de FIPS. • Al hacer clic en **Importar clave** o **Exportar clave** en **Propiedades de IPS** | **Administración de claves**, es necesario seleccionar el tipo de clave que se desea importar o exportar. • En el **Asistente de adición de dispositivos**, el protocolo TCP siempre está establecido en el puerto 22. El puerto SSH se puede cambiar.

Selección del modo FIPS

La primera vez que inicie sesión en el sistema, se le preguntará si desea que el sistema funcione en el modo FIPS o no. Una vez realizada la selección, no es posible cambiarla.

Procedimiento

Para ver las definiciones de las opciones, haga clic en **?** en la interfaz.

1 La primera vez que inicie sesión en ESM:

   a En el campo **Nombre de usuario**, escriba `NGCP`.

   b En el campo **Contraseña**, escriba `security.4u`.

   Se le pedirá que cambie su contraseña.

2 Introduzca y confirme la nueva contraseña.

3 En la página **Activar FIPS**, haga clic en **Sí**.

La advertencia de **Activar FIPS** mostrará información para solicitar confirmación de que desea que el sistema funcione en el modo FIPS de forma permanente.

4 Haga clic en **Sí** para confirmar su selección.

Comprobación de integridad de FIPS

Si utiliza el sistema en el modo FIPS, FIPS 140-2 requiere la comprobación de la integridad del software de forma regular. Esta comprobación se debe realizar en el sistema y en todos los dispositivos.

Procedimiento

Para ver las definiciones de las opciones, haga clic en **?** en la interfaz.

1 En el árbol de navegación del sistema, seleccione **Propiedades del sistema** y asegúrese de que esté seleccionada la opción **Información del sistema**.

2 Realice cualquiera de las acciones que se indican a continuación.

En este campo...	Haga esto...
Estado de FIPS	Visualice los resultados de la prueba automática de FIPS más reciente realizada en el ESM.
Prueba o **Prueba automática de FIPS**	Ejecute las pruebas automáticas de FIPS, las cuales comprueban la integridad de los algoritmos utilizados dentro del archivo ejecutable criptográfico. Los resultados se pueden ver en el **Registro de mensajes**. Si la prueba automática de FIPS falla, la seguridad de FIPS se ha visto comprometida o se ha producido algún fallo de dispositivo. Póngase en contacto con el Soporte de McAfee.
Ver o **Identidad de FIPS**	Abra la página **Token de identidad de FIPS** para realizar las pruebas de encendido de integridad del software. Compare el valor siguiente con la clave pública que aparece en esta página: -----BEGIN PUBLIC KEY----- MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAt8FWOP2mvVjvTTxkhGqk LdgA+sx0jBv+zYnCkGYOHHzNAdum9yuMn69GNbYXm7I5OcKv2+nz6axBruCZ5XX1 jCGWnmsj8YZJoNp/FLUy1jYE7lXI5/NRm2uhjhzjdOjgFv10SkgxVfL/aBJjqZFJ KKbHMzYEBwdyseQUc56u3mKaBtP4rydfRmEtytkuOsZgQuPHKYhaQJlnbV5LfrLa o6HQSlzHYHlcF/Yog+QHJ6ClSRA1lk8MPyFG9RHdKnwcq3sY8QjQMbIZ5SDobbK0 GPOOucG8vWDWdxSiabJLBdklVsmB0zwdH6lOCkkGTidayMk12hDh+2BA6el7YQBV 8EJaJ5wvz8aQKwDfiinlb9vmC+sk+Rwo/E7uRn3El4+RxouHi9J3f92I9qXZeJCV iYV2XahhyxSpq8ro/j0BMTiab3dIjjogxMxCI9QjEpm3J/ZyUpWtNKaHq8BgSE1e daiJob7O/kvef1T/ZOb3O90bSK3vtn+3Si3K3cpaY/qBm9var6xVNyGhHztRJv0F 0nSJlyddWuXL1U+hMTO2YE33T3s4Uf4jiomTVSDTJ087hLT5l/hCz6A33Hzl7gk8 Q89SNsmL/p0RAJzJ3+mGyoUAd1D2u6sYq6NkGCn640a5A2zAOQdX/M8R8S+NKjgi nLg3n+/+25KsCB3KDY3AkYECAwEAAQ== -----END PUBLIC KEY----- Si este valor y la clave pública no coinciden, la seguridad de FIPS se ha visto comprometida. Póngase en contacto con el Soporte de McAfee.

Adición de un dispositivo con clave aplicada en el modo FIPS

Existen dos métodos en el modo FIPS para agregar un dispositivo con una clave ya aplicada a un ESM. Estos términos y extensiones de archivo le resultarán útiles a la hora de realizar estos procesos.

Terminología

- **Clave de dispositivo**: contiene los derechos de administración que tiene un ESM para un dispositivo; no se emplea con fines criptográficos.
- **Clave pública**: la clave de comunicación SSH pública del ESM, que se almacena en la tabla de claves autorizadas de un dispositivo.
- **Clave privada**: la clave de comunicación SSH privada del ESM, utilizada por el ejecutable de SSH en un ESM a fin de establecer la conexión SSH con un dispositivo.
- **ESM principal**: el ESM utilizado originalmente para registrar el dispositivo.
- **ESM secundario**: un ESM adicional que se comunica con el dispositivo.

Extensiones de archivo de los distintos archivos de exportación

- **.exk**: contiene la clave de dispositivo.
- **.puk**: contiene la clave pública.
- **.prk**: contiene la clave privada y la clave de dispositivo.

Copia de seguridad y restauración de información de un dispositivo en modo FIPS

Este método se emplea para crear copias de seguridad de la información de comunicación de un dispositivo y restaurarlas en el ESM.

Está destinado principalmente a su uso en caso de un fallo que requiera la sustitución del ESM. Si la información de comunicación no se exporta antes del fallo, la comunicación con el dispositivo no se podrá restablecer. Este método exporta e importa el archivo .prk.

La clave privada del ESM principal es utilizada por el ESM secundario para establecer comunicación con el dispositivo inicialmente. Una vez establecida la comunicación, el ESM secundario copia su clave pública en la tabla de claves autorizadas del dispositivo. El ESM secundario borra entonces la clave privada del ESM principal e inicia la comunicación con su propio par de claves pública/privada.

Acción	Pasos
Exportar el archivo .prk del ESM principal	1 En el árbol de navegación del sistema del ESM principal, seleccione el dispositivo con la información de comunicación de la que desee crear una copia de seguridad y, después, haga clic en el icono **Propiedades**. 2 Seleccione **Administración de claves** y haga clic en **Exportar clave**. 3 Seleccione **Copia de seguridad de clave privada SSH** y haga clic en **Siguiente**. 4 Escriba y confirme una contraseña; a continuación, establezca la fecha de caducidad. Una vez que pasa la fecha de caducidad, la persona que importa la clave no se puede comunicar con el dispositivo hasta que se exporta otra clave con una fecha de caducidad futura. Si selecciona **No caduca nunca**, la clave no caducará al importarla a otro ESM. 5 Haga clic en **Aceptar**, seleccione la ubicación para guardar el archivo .prk creado por el ESM y cierre la sesión en el ESM principal.
Agregar un dispositivo al ESM secundario e importar el archivo .prk	1 En el árbol de navegación del sistema del dispositivo secundario, seleccione el nodo de nivel de sistema o grupo al que desee agregar el dispositivo. 2 En la barra de herramientas de acciones, haga clic en **Agregar dispositivo**. 3 Seleccione el tipo de dispositivo que desee agregar y haga clic en **Siguiente**. 4 Introduzca un nombre para el dispositivo exclusivo en el grupo y haga clic en **Siguiente**. 5 Introduzca la dirección IP de destino del dispositivo, indique el puerto de comunicación FIPS y haga clic en **Siguiente**. 6 Haga clic en **Importar clave**, desplácese hasta el archivo .prk y haga clic en **Cargar**. Escriba la contraseña especificada al exportar esta clave inicialmente. 7 Cierre la sesión en el ESM secundario.

Activación de la comunicación con varios dispositivos ESM en el modo FIPS

Es posible permitir que diversos ESM se comuniquen con el mismo dispositivo mediante la exportación e importación de archivos .puk y .exk.

En este método se usan dos procesos de exportación e importación. En primer lugar, se usa el ESM principal para importar el archivo .puk exportado del dispositivo ESM secundario y enviar la clave pública del ESM secundario al dispositivo, lo cual permite que ambos dispositivos ESM se comuniquen con el dispositivo. En segundo lugar, el archivo .exk del dispositivo se exporta desde el ESM principal y se importa en el ESM secundario, lo cual permite al ESM secundario comunicarse con el dispositivo.

Acción	Pasos
Exportar el archivo .puk del ESM secundario	1 En la página **Propiedades del sistema** del ESM secundario, seleccione **Administración de ESM**. 2 Haga clic en **Exportar SSH** y, después, seleccione la ubicación para guardar el archivo .puk. 3 Haga clic en **Guardar** y cierre la sesión.
Importar el archivo .puk al ESM principal	1 En el árbol de navegación del sistema del ESM principal, seleccione el dispositivo que desee configurar. 2 Haga clic en el icono **Propiedades** y seleccione **Administración de claves**. 3 Haga clic en **Administrar claves SSH**. 4 Haga clic en **Importar**, seleccione el archivo .puk y haga clic en **Cargar**. 5 Haga clic en **Aceptar** y cierre la sesión en el ESM principal.
Exportar el archivo .exk del dispositivo del ESM principal	1 En el árbol de navegación del sistema del ESM principal, seleccione el dispositivo que desee configurar. 2 Haga clic en el icono **Propiedades** y seleccione **Administración de claves**. 3 Haga clic en **Exportar clave**, seleccione la clave del dispositivo de copia de seguridad y haga clic en **Siguiente**. 4 Escriba y confirme una contraseña; a continuación, establezca la fecha de caducidad. Una vez que pasa la fecha de caducidad, la persona que importa la clave no se puede comunicar con el dispositivo hasta que se exporta otra clave con una fecha de caducidad futura. Si selecciona **No caduca nunca**, la clave no caducará al importarla a otro ESM. 5 Seleccione los privilegios del archivo .exk y haga clic en **Aceptar**. 6 Seleccione la ubicación para guardar el archivo y cierre la sesión en el ESM principal.
Importar el archivo .exk en el ESM secundario	1 En el árbol de navegación del sistema del dispositivo secundario, seleccione el nodo de nivel de sistema o grupo al que desee agregar el dispositivo. 2 En la barra de herramientas de acciones, haga clic en **Agregar dispositivo**. 3 Seleccione el tipo de dispositivo que desee agregar y haga clic en **Siguiente**. 4 Introduzca un nombre para el dispositivo que sea exclusivo en el grupo y haga clic en **Siguiente**. 5 Haga clic en **Importar clave** y busque el archivo .exk. 6 Haga clic en **Cargar** y escriba la contraseña especificada al exportar esta clave inicialmente. 7 Cierre la sesión en el ESM secundario.

Solución de problemas del modo FIPS

Es posible que surjan problemas al utilizar el ESM en el modo FIPS.

Problema	Descripción y solución
No hay comunicación con el ESM	• Compruebe la pantalla LCD situada en la parte delantera del dispositivo. Si indica **Fallo de FIPS**, póngase en contacto con el Soporte de McAfee. • Busque una situación de error en la interfaz HTTP; para ello, acceda a la página web Prueba automática de FIPS de ESM mediante un navegador. - Si aparece únicamente el dígito **0**, el cual indica que el dispositivo ha fallado una prueba automática de FIPS, reinicie el dispositivo ESM para intentar corregir el problema. Si el fallo persiste, póngase en contacto con el servicio de Soporte para obtener instrucciones adicionales. - Si aparece únicamente el dígito **1**, el problema de comunicación no se debe a un fallo de FIPS. Póngase en contacto con el Soporte técnico para obtener instrucciones adicionales.
No hay comunicación con el dispositivo	• Si hay una marca de estado junto al dispositivo en el árbol de navegación del sistema, coloque el cursor sobre él. Si indica **Fallo de FIPS**, póngase en contacto con el Soporte de McAfee a través del portal de soporte. • Siga la descripción correspondiente al problema *No hay comunicación con el ESM*.
Error **El archivo no es válido** al agregar un dispositivo	No se puede exportar una clave de un dispositivo no FIPS e importarla a un dispositivo que funcione en el modo FIPS. De igual forma, no se puede exportar una clave de un dispositivo FIPS e importarla a un dispositivo no FIPS. Este error aparece cuando se intenta cualquiera de estas dos cosas.

B Requisitos de ESXi para máquinas virtuales

La máquina virtual debe ajustarse a los siguientes requisitos mínimos.

- Procesador: de 8 núcleos o más según el modelo, 64 bits, Dual Core2/Nehalem o superior, o bien AMD Dual Athlon64/Dual Opteron64 o posterior
- RAM: depende del modelo (4 GB o más)
- Disco: depende del modelo (250 GB o más)
- ESXi: 5.0 o posterior

Puede seleccionar el espacio libre en el disco duro necesario para el servidor. Sin embargo, los requisitos de la máquina virtual dependen del modelo del dispositivo (250 GB o más). Si no cuenta con un mínimo de 250 GB disponibles, recibirá un error al desplegar la máquina virtual.

La máquina virtual hace uso de diversas funciones que requieren CPU y RAM. Si el entorno ESXi comparte de alguna forma los requisitos de CPU/RAM con otras máquinas virtuales, el rendimiento de la máquina virtual se verá afectado. Planifique las necesidades de CPU y RAM de acuerdo con los requisitos aquí indicados.

McAfee recomienda configurar la opción de aprovisionamiento con el valor **Thick** (Grueso).

Contenido

- *Modelos de máquina virtual*
- *División de la unidad de almacenamiento*
- *Instalación de la máquina virtual*
- *Configuración de la máquina virtual*
- *Aplicación de una clave al dispositivo de máquina virtual*

Modelos de máquina virtual

En esta tabla se indican los modelos de máquina virtual disponibles, cuántos eventos por segundo (EPS) puede procesar cada modelo, el almacenamiento mecánico recomendado, la capacidad de

almacenamiento de la unidad de estado sólido (SSD) y los requisitos correspondientes a la plataforma donde se ejecuta la máquina virtual.

Número de modelo	Capacidad de EPS	Almacenamiento mecánico	SSD	Requisitos de plataforma
ELU4 ELU12	1000 5000	Entorno de máquina virtual recomendado de 250 GB Máquina virtual recomendada Entorno de 500 GB como mínimo	Ninguna Mínimo de 240 GB	VMware ESX/ESXi Server v.5.x +, procesador de 8 núcleos (Intel® Xeon® Processor E5 o E7), 4 GB de memoria VMware ESX/ESXi Server v.5.x +, procesador de 12 núcleos (Intel® Xeon® Processor E5 o E7), 64 GB de memoria
ENU4 ENU12 ENU32	1500* 40 000* 85 000*	Entorno de máquina virtual recomendado de 250 GB Entorno de máquina virtual recomendado de 500 GB mínimo Entorno de máquina virtual recomendado de 2 TB mínimo	Ninguna Mínimo de 480 GB Mínimo de 3 TB	VMware ESX/ESXi Server v.5.x +, procesador de 8 núcleos (Intel® Xeon® Processor E5 o E7), 4 GB de memoria VMware ESX/ESXi Server v.5.x +, procesador de 12 núcleos (Intel® Xeon® Processor E5 o E7), 64 GB de memoria VMware ESX/ESXi Server v.5.x +, procesador de 32 núcleos (Intel® Xeon® Processor E5 o E7), 96 GB de memoria
ELM4 ELM12 ELM32	1500* 30 000* 70 000*	Entorno de máquina virtual recomendado de 250 GB Entorno de máquina virtual recomendado de 500 GB mínimo Entorno de máquina virtual recomendado de 2 TB mínimo	Ninguna Mínimo de 480 GB Mínimo de 3 TB	VMware ESX/ESXi Server v.5.x +, procesador de 8 núcleos (Intel® Xeon® Processor E5 o E7), 4 GB de memoria VMware ESX/ESXi Server v.5.x +, procesador de 12 núcleos (Intel® Xeon® Processor E5 o E7), 64 GB de memoria VMware ESX/ESXi Server v.5.x +, procesador de 32 núcleos (Intel® Xeon® Processor E5 o E7), 96 GB de memoria
EV2 EV5 EV10	500 5000 15 000	Entorno de máquina virtual recomendado de 250 GB Entorno de máquina virtual recomendado de 500 GB mínimo Entorno de máquina virtual recomendado de 2 TB mínimo	Ninguna Mínimo de 480 GB Mínimo de 3 TB	VMware ESX/ESXi Server v.5.x +, procesador de 8 núcleos (Intel® Xeon® Processor E5 o E7), 4 GB de memoria VMware ESX/ESXi Server v.5.x +, procesador de 12 núcleos (Intel® Xeon® Processor E5 o E7), 64 GB de memoria VMware ESX/ESXi Server v.5.x +, procesador de 32 núcleos (Intel® Xeon® Processor E5 o E7), 96 GB de memoria

Número de modelo	Capacidad de EPS	Almacenamiento mecánico	SSD	Requisitos de plataforma
ELMERCVM4 ELMERCVM12	1500 5000	Entorno de máquina virtual recomendado de 250 GB Entorno de máquina virtual recomendado de 500 GB mínimo	Ninguna Mínimo de 240 GB	VMware ESX/ESXi Server v.5.x +, procesador de 8 núcleos (Intel® Xeon® Processor E5 o E7), 4 GB de memoria VMware ESX/ESXi Server v.5.x +, procesador de 12 núcleos (Intel® Xeon® Processor E5 o E7), 64 GB de memoria
ACV12 ACV32	<30 000* <80 000*	Entorno de máquina virtual recomendado de 250 GB Entorno de máquina virtual recomendado de 500 GB mínimo	Mínimo de 480 GB Mínimo de 3 TB	VMware ESX/ESXi Server v.5.x +, procesador de 12 núcleos (Intel® Xeon® Processor E5 o E7), 64 GB de memoria VMware ESX/ESXi Server v.5.x +, procesador de 32 núcleos (Intel® Xeon® Processor E5 o E7), 96 GB de memoria
APM4 APM12	250 Mbps 500 Mbps	Entorno de máquina virtual recomendado de 250 GB Entorno de máquina virtual recomendado de 500 GB mínimo	Ninguna Mínimo de 480 GB	VMware ESX/ESXi Server v.5.x +, procesador de 8 núcleos (Intel® Xeon® Processor E5 o E7), 4 GB de memoria VMware ESX/ESXi Server v.5.x +, procesador de 12 núcleos (Intel® Xeon® Processor E5 o E7), 64 GB de memoria

División de la unidad de almacenamiento

Si el modelo tiene más de 250 GB y necesita usar la configuración **256 MB to 2 GB** (De 256 MB a 2 GB), deberá dividir la unidad de almacenamiento de la máquina virtual.

Procedimiento

1 Seleccione el servidor ESX, haga clic en la ficha **Configuration** (Configuración) y, después, en **Storage** (Almacenamiento) en la sección **Hardware** (Hardware).

La máquina virtual hace uso de diversas funciones que requieren CPU y RAM. Si el entorno ESXi comparte los requisitos de CPU/RAM con otras máquinas virtuales, el rendimiento de la máquina virtual se verá afectado. Planifique la capacidad de CPU y RAM de acuerdo con los requisitos.

2 Haga clic en **Add Storage** (Agregar almacenamiento) y, después, seleccione **Disk/LUN** (Disco/LUN).

3 Seleccione un disco disponible y, después, seleccione la opción correcta para el espacio libre en disco: **Use 'Free space'** (Usar "espacio libre") en el caso de una unidad existente o **Use all available partitions** (Usar todas las particiones disponibles) en el caso de una unidad.

Puede seleccionar el espacio libre en el disco duro necesario para el servidor, pero el requisito correspondiente a la máquina virtual es 500 GB. Si no cuenta con 500 GB disponibles, recibirá un error al desplegar la máquina virtual. McAfee recomienda configurar el aprovisionamiento con el valor **Thick** (Grueso).

4 Asigne un nombre a la unidad de almacenamiento y, después, seleccione **512 GB, Block size: 2 MB** (512 GB, tamaño de bloque: 2 MB) en la lista desplegable **Maximum file size** (Tamaño máximo de archivo) para asegurarse de disponer de los 500 GB de espacio libre en la unidad.

Instalación de la máquina virtual

Tras instalar y aplicar la clave a una máquina virtual, esta imita el funcionamiento normal de ESM.

Antes de empezar

Compruebe que su equipo se ajuste a los requisitos mínimos.

Procedimiento

1 Acceda a la raíz de la unidad de CD (para la instalación mediante CD) o descargue los archivos proporcionados por el Soporte de McAfee en el equipo local.

2 En **vSphere Client** (Cliente vSphere), haga clic en la IP del servidor en el árbol de dispositivos.

3 Haga clic en **File** (Archivo) y seleccione **Deploy OVF Template** (Desplegar plantilla OVF).

4 Designe el nombre, la carpeta para instalar la máquina virtual, la configuración de aprovisionamiento de disco y la opción **VM Networking** (Red de máquina virtual).

5 Despliegue los archivos en el servidor ESXi, seleccione la máquina virtual y asegúrese de que lo siguiente esté establecido en la opción **Edit Virtual Machine** (Editar máquina virtual).

6 Seleccione la configuración de red correcta para sus conmutadores/adaptadores de red ESXi y, después, haga clic en **Play** (Ejecutar) para iniciar la máquina virtual.

7 Mediante el menú de la máquina virtual, establezca la IP de administración 1, la máscara de red, el gateway y las direcciones DNS; a continuación, pulse **Esc** para activar el menú.

8 Configure la interfaz de red en la máquina virtual, guarde los cambios antes de salir de la ventana **Menu** (Menú) y aplique la clave al dispositivo.

Configuración de la máquina virtual

Una vez instalada la máquina virtual, deberá configurar la interfaz de red.

Procedimiento

1 Haga clic en **Esc**, desplácese hacia abajo hasta **MGT IP Conf** (Conf. IP admin.) en la pantalla LCD y haga clic en **Intro** dos veces.

2 Establezca la dirección IP utilizando las flechas para cambiar el valor del dígito activo y para pasar de un dígito a otro; a continuación, haga clic en **Intro**.

3 Desplácese hasta **Netmask** (Máscara de red) y establezca el valor mediante las flechas.

4 Desplácese hasta **Done** (Listo) y haga clic en **Intro**. Después, desplácese hacia abajo hasta **Gateway** (Gateway) y haga clic en **Intro**.

5 Establezca la dirección del gateway a través de las flechas, desplácese hacia abajo hasta **Done** (Listo) y pulse **Intro**.

6 Desplácese hacia abajo hasta **DNS1** (DNS 1), pulse **Intro** y seleccione la dirección del servidor DNS mediante las flechas.

7 Desplácese hacia abajo hasta **Done** (Listo) y pulse **Intro**.

8 Para cambiar el puerto de comunicación cuando el sistema funcione en el modo FIPS (véase *Acerca del modo FIPS*), pulse la flecha hacia abajo dos veces y, después, pulse **Intro**.

No cambie el puerto de comunicación TCP.

9 Cambie el número de puerto y pulse **Intro**.

Tome nota del nuevo número de puerto. Introdúzcalo en el momento de aplicar la clave al dispositivo.

10 Desplácese hasta **Save Changes** (Guardar cambios) y haga clic en **Intro**.

Aplicación de una clave al dispositivo de máquina virtual

Es necesario aplicar una clave al dispositivo para establecer un vínculo entre el dispositivo y el ESM.

Antes de empezar

Conecte físicamente el dispositivo a la red (véase *Instalación de los dispositivos McAfee ESM*).

Procedimiento

Para ver las definiciones de las opciones, haga clic en **?** en la interfaz.

1 En el árbol de navegación del sistema, haga clic en un sistema o un grupo y, después, en el icono **Agregar dispositivo** del panel de acciones.

2 Introduzca la información solicitada en cada una de las páginas del **Asistente de adición de dispositivos** (véase *Adición de dispositivos a la consola de ESM* en la *Guía del producto de McAfee Enterprise Security Manager*).

C Instalación de los adaptadores SAN qLogic 2460 o 2562

El qLogic QLE2460 es un adaptador único de canal de fibra PCIe x4 de 4 GB. El qLogic QLE2562 es un adaptador único de canal de fibra PCIe x8 de 8 GB. Se pueden conectar directamente al dispositivo SAN o a través de un conmutador SAN.

Antes de empezar

- Asegúrese de que el dispositivo o el conmutador SAN que se van a conectar lleven a cabo la negociación automática.
- Asegúrese de que el administrador de SAN asigne y cree espacio en el SAN, además de asignarlo al canal donde esté conectado el adaptador qLogic. Use el nombre de puerto WWPN para el adaptador. El WWPN se encuentra en la tarjeta del adaptador, en la bolsa antiestática y en la caja.

Procedimiento

1 Apague el dispositivo en el que vaya a instalar el adaptador SAN.

2 Inserte el adaptador, coloque el dispositivo de nuevo en el bastidor y conecte los cables.

En el caso de los dispositivos 3U, inserte el adaptador en la ranura más cercana a la cubierta protectora de la memoria.

El mensaje de arranque de la BIOS del adaptador informará de que el adaptador está instalado y en funcionamiento. Si no aparece este mensaje o si la tarjeta no presenta luces rojas, amarillas o verdes, significa que la tarjeta no se reconoce. De ser así, asegúrese de que la tarjeta esté bien colocada o insértela en una ranura PCI distinta.

3 Inicie el dispositivo.

El entorno operativo llevará a cabo la detección y cargará el controlador QLAXXX. El mensaje **Mounting Storage Facilities** (Servicios de almacenamiento de montaje) mostrará **OK** (Aceptar) y el inicio continuará.

4 Mediante la consola de ESM, aplique la clave al dispositivo.

Una vez que el dispositivo tenga la clave aplicada, la página **Propiedades** incluirá la opción **Volúmenes SAN**.

D Instalación del DAS

El DAS es un dispositivo complementario para un ELM o un ESM de las series 4xxx/5xxx/6xxx.

La unidad DAS se suministra con un chasis y una tarjeta RAID LSI 9280-8e para:

- ETM-5205
- ETM-5510
- ETM-5600
- ETM-5750
- ETM-6000
- ETM-X3
- ETM-X4
- ETM-X5
- ETM-X6
- ESMREC-5205
- ESMREC-5510
- ENMELM-4600
- ENMELM-5205
- ENMELM-5510
- ENMELM-5600
- ENMELM-6000
- ELM-4600
- ELM-5205
- ELM-5510
- ELM-5600
- ELM-5750
- ELM-6000

Procedimiento

1. Encienda el ESM tras un procedimiento de cierre normal.
2. Saque el dispositivo del bastidor y abra la cubierta superior. Puede que necesite retirar un pequeño tornillo situado en la parte delantera o trasera de la cubierta.
3. Instale la tarjeta RAID LSI 9280-8e en la ranura 4 del ESM.
   - En el caso de los dispositivos con el frontal naranja, si la tarjeta RAID Areca o 3Ware está en la ranura 4, mueva esa tarjeta RAID a la ranura 6. Si el dispositivo McAfee ESM tiene instaladas tanto una tarjeta RAID Areca o 3Ware como una tarjeta SSD, instale la tarjeta RAID LSI 9280-8e en la ranura 5.
   - En los dispositivos con el frontal negro, instale la tarjeta en una ranura libre.
4. Vuelva a colocar la cubierta del dispositivo McAfee ESM e insértelo de nuevo en el bastidor.
5. Inserte los conectores de cable en las ranuras 1 y 2 correspondientes a las ranuras externas de la tarjeta RAID LSI 9280-8e. Al colocar el cable en su sitio, se producirá un chasquido.
6. Verifique que todas las unidades estén bien insertadas en el DAS y, después, coloque los rieles internos en el dispositivo DAS e insértelo en el bastidor.
7. Inserte los cables de datos en las ranuras primera y tercera de la parte posterior del dispositivo DAS. Al colocar los cables en su sitio, se producirá un chasquido.

8 Inserte los cables de alimentación y, después, encienda el dispositivo DAS.

9

Aparecerá una luz de prueba para todas las unidades. La unidad con la luz roja corresponde a la "reserva activa" para el DAS.

10 Encienda el dispositivo McAfee ESM y busque la utilidad BIOS de la tarjeta RAID LSI 9280-8e.

El dispositivo DAS ya dispone de formato y no requiere la configuración de un conjunto de discos RAID. Si ve un mensaje que indica que **RAID no está presente**, póngase en contacto con el Soporte de McAfee para crear el RAID.

11 Inicie sesión y ejecute el comando `df -h` para asegurarse de tener una unidad /das1_hd.

En la página **Propiedades del sistema** de la consola de ESM, el campo **Hardware** de la página **Información del sistema** refleja el aumento de tamaño de la unidad de disco duro con la etiqueta /data_hd.

E

Instalación de los dispositivos en un bastidor

Se recomienda instalar los dispositivos en un bastidor para proteger tanto los dispositivos como el cableado de daños o desconexiones accidentales.

Contenido

- *Instalación del juego de rieles AXXVRAIL*
- *Extracción del chasis*

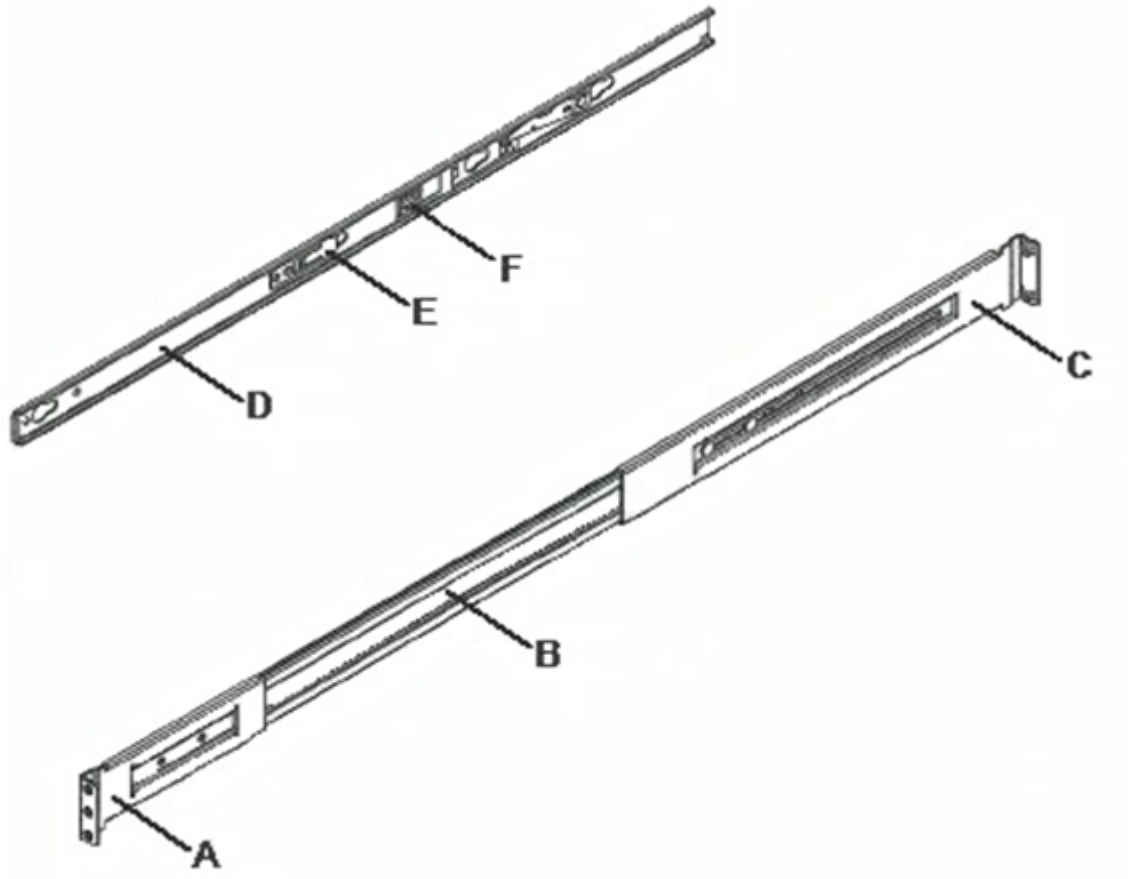
Instalación del juego de rieles AXXVRAIL

Junto con cada dispositivo, se incluye un juego de rieles AXXVRAIL para la instalación en un bastidor.

Procedimiento

1 Instale los rieles en el bastidor.

a Tire del botón de liberación (F) a fin de retirar el elemento interno (D) de la corredera.



Componentes

A - Lengüeta delantera

B - Elemento exterior

C - Lengüeta trasera

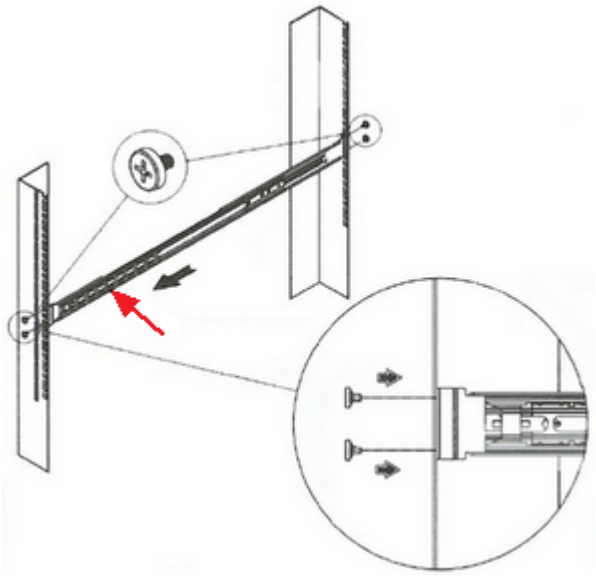
D - Elemento interior

E - Pasador de bloqueo de seguridad

F - Botón de liberación

b Alinee las lengüetas en la posición vertical que prefiera en el bastidor y, después, inserte los tornillos.

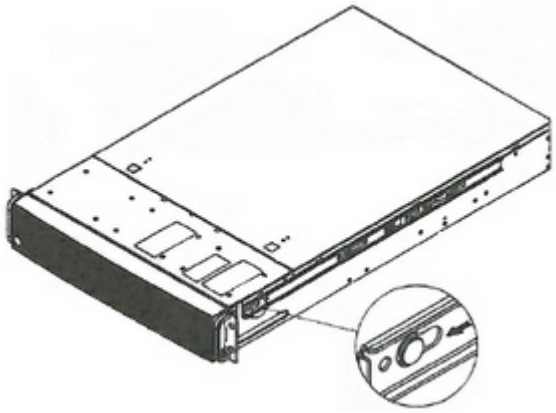
c Mueva el retén a la parte delantera de la corredera.



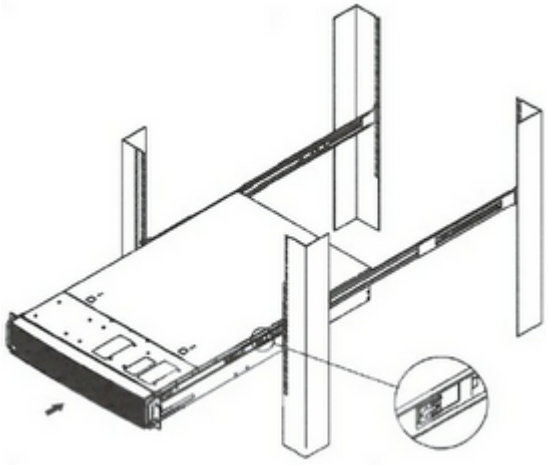
2 Instale el chasis.

a Alinee los agujeros del elemento interior con los separadores del chasis.

b Mueva el elemento interior en la dirección mostrada en la imagen siguiente.



c Instale el chasis en las correderas fijas; para ello, tire del botón de liberación del elemento interior a fin de desbloquearlo y coloque el chasis en su sitio.



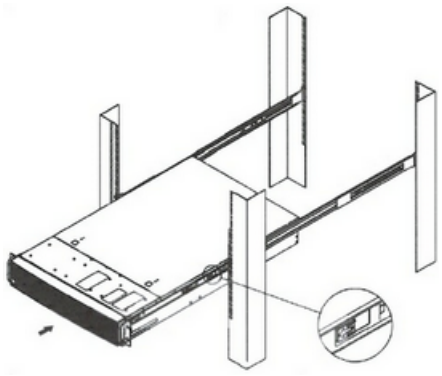
Extracción del chasis

Es posible sacar el chasis de los rieles.

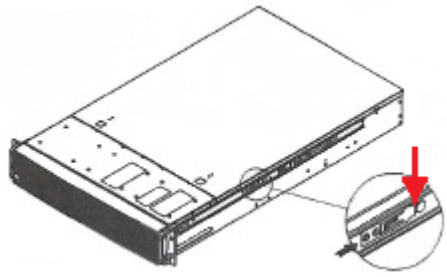
Procedimiento

1 Extienda al máximo las correderas hasta que se bloqueen.

2 Tire del botón de liberación a fin de soltar el bloqueo y desconecte el elemento interior de la corredera.



3 Empuje la clavija de bloqueo de seguridad para soltar el elemento interior del chasis.



F

Avisos normativos

La siguiente información sobre normativas se aplica a las distintas plataformas que se pueden emplear.

Tabla F-1 Plataformas basadas en SuperMicro

	McAfee 1U	McAfee 2U o 3U
Emisiones electromagnéticas	FCC Clase B, EN 55022 Clase B, EN 61000-3-2/-3-3 CISPR 22 Clase B	FCC Clase B, EN 55022 Clase B, EN 61000-3-2/-3-3 CISPR 22 Clase B
Inmunidad electromagnética	EN 55024/CISPR 24, (EN 61000-4-2, EN 61000-4-3, EN 61000-4--4, EN 61000-4-5, EN 61000-4-6, EN 61000-4-8, EN 61000-4-11) 55024	EN 55024/CISPR 24, (EN 61000-4-2, EN 61000-4-3, EN 61000-4--4, EN 61000-4-5, EN 61000-4-6, EN 61000-4-8, EN 61000-4-11) 55024
Seguridad	EN 60950/Conforme con IEC 60950, Certificación UL (EE. UU.) Certificación CUL (Canadá) Certificación TÜV (Alemania) Marcado CE (Europa)	EN 60950/Conforme con IEC 60950, Certificación UL (EE. UU.) Certificación CUL (Canadá) Certificación TÜV (Alemania) Marcado CE (Europa)

Tabla F-2 Plataformas basadas en DAS

	DAS-50, DAS-100
Tensión de entrada	100/240 Vca
Frecuencia de entrada	50/60 Hz
Fuente de alimentación	1400 W X3
Consumo de energía	472 W a 120 Vca 461 W a 240 Vca
Amperios (máx.)	9,4 A
Altitud (máx.)	De -0,01 a 3 km
Temperatura (máx.)	De 10º a 35º C (en funcionamiento) De -40º a 70º C (en reposo)
Altitud	De -0,01 a 3 km (en funcionamiento) y de -0,01 a 7,60 km (en reposo)

Tabla F-2 Plataformas basadas en DAS *(continuación)*

	DAS-50, DAS-100
Vatios	471,27
Humedad	En funcionamiento: del-10 % al 85 % (sin condensación) En reposo: del -10 % al 90 %

Tabla F-3 Plataformas basadas en Intel 1U

Parámetro	Límites
Temperatura de funcionamiento	De +10° C a +35° C con una tasa máxima de variación no superior a 10° C por hora
Temperatura en reposo	De -40° C a +70° C
Humedad en reposo	90 % sin condensación a 35° C
Ruido acústico	Potencia de sonido: 7,0 BA en estado inactivo con temperatura ambiente de oficina normal (23 +/- 2º C)
Impacto en funcionamiento	Semionda sinusoidal, pico de 2 g, 11 ms
Impacto sin embalaje	Trapezoidal, 25 g, cambio de velocidad de 345,44 cm/s (de ≧18,14 kg a >36,29 kg)
Impacto con embalaje	Caída libre sin paletizar de 61 cm (de ≧18,14 kg a >36,29 kg)
Impacto en funcionamiento	Semionda sinusoidal, pico de 2 g, 11 ms
Vibración sin embalaje	De 5 Hz a 500 Hz, 2,20 g RMS aleatorio
DES	+/-12 kV en descarga aérea y 8 K por contacto
Requisito de refrigeración del sistema en vatios	486,50 W

Tabla F-4 Plataformas basadas en Intel 2U

Parámetro		Límites
Temperatura	Funcionamiento	• ASHRAE Clase A2: funcionamiento continuo. De 10° C a 35° C con un tasa máxima de variación no superior a 10° C por hora. • ASHRAE Clase A3: incluye funcionamiento hasta 40° C un máximo de 900 horas al año • ASHRAE Clase A4: incluye funcionamiento hasta 45° C un máximo de 90 horas al año
	Envío	De -40° C a 70° C
Altitud (funcionamiento)		Admite el funcionamiento hasta 3050 m con reducciones de capacidad de clase ASHRAE
Humedad (envío)		Del 50 % al 90 % sin condensación, con un máximo en termómetro húmedo de 28° C (a temperaturas de entre 25° C y 35° C)
Impacto	Funcionamiento	Semionda sinusoidal, 2 g, 11 ms
	Sin embalaje	Trapezoidal, 25 g, la variación de velocidad se basa en el peso con embalaje

Tabla F-4 Plataformas basadas en Intel 2U *(continuación)*

Parámetro		Límites
	Con embalaje	Peso del producto: de ≥40 a <80 Altura de caída libre sin paletizar = 45,72 cm Altura de caída libre paletizado (producto único) = N/D
Vibración		De 5 Hz a 500 Hz 2,20 g RMS aleatorio
	Con embalaje	De 5 Hz a 500 Hz 1,09 g RMS aleatorio
CA-CC	Tensión	De 90 V a 132 V y de 180 V a 264 V
	Frecuencia	De 47 Hz a 63 Hz
	Interrupción de alimentación	No hay pérdida de datos si se corta la alimentación hasta 12 ms
	Sobretensión en reposo y en funcionamiento	Unidireccional

Índice

A

ACE, configurar interfaz de red 24
acerca de esta guía 5
adaptador SAN, instalar 43
ADM, configurar interfaz de red 24
avisos normativos para plataformas 53
AXXVRAIL, rieles
    extraer chasis 51
    instalar 48

C

cables de red, identificar 12
conectar dispositivo 11
configurar interfaz de red
    ACE 24
    ELM 24
    Event Receiver 24
contraseña de la consola de ESM 26
convenciones tipográficas e iconos utilizados en esta guía 5

D

DAS, instalar 45
DEM, configurar interfaz de red 24
dispositivos
    conectar 11
    configurar 23
    iniciar 11
dispositivos, inspeccionar 10
documentación
    convenciones tipográficas e iconos 5
    destinatarios de esta guía 5
    específica de producto, buscar 6

E

ELM, configurar interfaz de red 24
embalaje, inspeccionar 10
ESM, configurar interfaz de red 25
exportar e importar
    archivo .exk 33
    archivo .puk 33
extensiones de archivo de archivos de exportación 32

F

FIPS
    activar 26
FIPS, modo
    dispositivo con clave aplicada, agregar 32
    extensiones de archivo 32
    terminología 32

H

hardware, requisitos mínimos 9

I

identificar cables de red 12
identificar puertos de red en dispositivos 13
iniciar dispositivo 11
iniciar sesión en la consola de ESM 26
inspeccionar embalaje y dispositivo 10
instalar
    identificar ubicación 10
instalar dispositivo
    preparativos 9
interfaz de red
    configurar en DEM y ADM 24
    configurar en ESM 25
    configurar en Nitro IPS 23
IPv6, configurar 26

M

máquina virtual
    aplicar clave 41
    configurar 40
    dividir unidad de almacenamiento 39
    instalar 40
    requisitos 37
McAfee ServicePortal, acceso 6
Modelos de máquina virtual 37
modo FIPS
    activar 30
    comprobar integridad 31
    comunicar con varios dispositivos ESM 33
    copia de seguridad de información 32
    funciones disponibles no conformes 30
    funciones eliminadas 30

modo FIPS *(continuación)*
funciones solo disponibles en el modo FIPS 30
restaurar información 32
seleccionar 30
solucionar problemas 35

N

Nitro IPS, configurar interfaz de red 23
nombre de usuario de la consola de ESM 26

P

plataformas, avisos normativos 53
puertos de red, identificar en cada dispositivo 13

Q

qLogic 2460, instalar adaptador SAN 43

R

receptor, configurar interfaz de red 24
red, identificar puertos de cada dispositivo 13
Requisitos de la máquina virtual 37
requisitos mínimos de hardware y software 9

S

ServicePortal, buscar documentación del producto 6
software, requisitos mínimos 9
solucionar problemas del modo FIPS 35
soporte técnico, encontrar información de productos 6

T

tipo de conector, identificar 12
tipo de equipo, identificar 12

U

ubicación de instalación 10